COMMENTS ON EDPB'S RECOMMENDATIONS 01/2020

on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

December, 20th 2020

The CJEU's "Schrems II" judgment has broad implications on the transfer of personal data from private entities or public bodies to third countries. Given the set of transfer tools provided by the GDPR and their respective characteristics, controllers, which had previously relied on the European Commission's adequacy decision following Art. 45 GDPR, are likely to switch to standard contractual clauses (SCCs) according to Art. 46(2)(c) GDPR or have already done so. While invalidating the Privacy Shield, the CJEU considers the SCCs still valid. However, the Court stated the requirement for data exporters and importers to verify whether supplementary measures are necessary given the prevailing position in a particular third country.

As a DPO, I strongly welcome EDPB's approach of supporting data exporters with detailed guidelines on how to scrutinize their transfers and especially on how to implement supplementary measures to SCCs. In order to be practical and helpful in a wide range of application scenarios, I would like to propose some additional clarifications in the recommendations.

I hope my modest contribution will help to further improve the comprehensibility and usefulness of your work.

Section 2.3

Step 3 of the recommendations (p. 12 et seq.) provides instructions on how to assess the effectiveness of the chosen transfer tool with respect to the legal situation in the respective country.

- As far as I understand the Schrems II decision, the Court does neither refer to particular types of processing, nor particular categories of personal data and data subjects.

  If the EDPB shares this interpretation, it should make clear that the verification (on whether the level of protection for personal data in a third country is "essentially equivalent" to that guaranteed in the EEA) can be made solely by looking at the *applicable law and current practice of the third country in general*[1]. Especially, it should be emphasized that – at least in this step – there is *no weighing of the risks*[2] to the rights and freedoms of natural persons involved *in the concrete data processing*.

- If the EDPB does not share this interpretation, it would be helpful to have further explanations and examples of *how the risks* (caused by a non-equivalent level of protection) to the rights and freedoms (in a concrete data processing) *are weighed*. In particular:

[1] Which may nevertheless depend on the purpose or categories of data etc. as these determine the domain of the processing (e.g. processing of telecommunication or medical data). This is already mentioned in paragraph 33.
[2] E.g. comparable to the weighing according to Art. 6(1)(f) or Art. 32 GDPR.

Which *factors* have to be considered when assessing the risks? E.g. should the possibility be included that public authorities not only gain access to the data transferred by the data exporter, but are also able to link it to data obtained from other processors or by surveilling Internet traffic?

- In both cases: Which transfers of personal data[3], if any, to third countries (in particular the U.S.) *under the SCCs without supplementary measures are still considered as lawful by the EDPB*?

Section 2.4

Assume a situation where the data exporter decides to adopt supplementary measures to the SCCs after its assessment in step 3:

- It should be clarified whether the requirement of reaching an "essentially equivalent level of protection" after adopting supplementary measures applies to *every category* of personal data (including meta data) involved in the processing.

  In Use Case 1, personal data is encrypted prior to transmission using key material under the sole control of the data exporter. Consider e.g. a company based in the EU which uses a web-based service for cloud storage located in a third country: inevitably. In order to provide the service, some personal data still has to be accessible by the data importer (and therefore by public authorities in its country) – at least login names and passwords, IP addresses, and browser fingerprints of the data exporter's employees using the cloud service.

  In the view of the EDPB: does the data exporter have to adopt additional measures[4] in order to protect the beforementioned categories of data as well?

And more generally:

- Does the EDPB follow the rather far-reaching opinion of the German Datenschutzkonferenz (expressed in its recent guide on videoconferencing systems[5]) that it is *difficult to imagine sufficient supplementary measures in situations where at least certain framework data[6] must be accessible to a provider for technical reasons*?

  If so, the EDPB's recommendations should very clearly indicate this and explain in which use cases (those mentioned in Annex 2 or additional ones) such a situation (where personal framework data must be accessible) may arise and how it should be dealt with.

---

[3] Consider e.g. the situation where a cloud service is used in a way that only the users' IP addresses (but not their names or e-mail addresses) are disclosed to the service provider.

[4] e.g. by using only pseudonymous logins and ensuring anonymous browsing

[5] https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf, p. 17: "Wenn das unzureichende Schutzniveau aus behördlichen Zugriffsmöglichkeiten herrührt, sind ausreichende zusätzliche Maßnahmen im Bereich von Videokonferenzdiensten schwer denkbar, denn mindestens bestimmte Rahmendaten der Konferenzen müssen dem Anbieter aus technischen Gründen zugänglich sein."

[6] Framework data ("Rahmendaten", cf. p. 4 of the guide) is described as metadata accruing while carrying out the communication, data about professional contacts, about working hours and work performance: "Weiterhin können Metadaten über die Durchführung der Kommunikation, Daten über die beruflichen Kontakte, über Arbeitszeiten und über die Arbeitsleistung anhand der Daten einer oder mehrerer Videokonferenzen verarbeitet werden (Rahmendaten)."